UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/803,120	03/17/2004	Brian D. Cunningham	Whit01	5291

33422 7590 04/01/2008

GOODMAN, ALLEN & FILETTI PLLC
4501 HIGHWOODS PARKWAY
SUITE 210
GLEN ALLEN, VA 23060

EXAMINER	
KESSLER, MATTHEW E	

ART UNIT	PAPER NUMBER
2145	

MAIL DATE	DELIVERY MODE
04/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/803,120	CUNNINGHAM, BRIAN D.	
	Examiner	Art Unit	
	Matthew E. Kessler	2145	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08). Paper No(s)/Mail Date *2/29/2008, 4/6/2006, 4/4/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 are pending.

2. Claims 1-30 are rejected.

Claim Objections

The following Claims are objected to because of the following informalities:

Claims 1, 5, and 8 all recite the limitation "means for receiving a confirmation request from said **sending device**." Then sending device does not send a confirmation request, however it does receive a confirmation request which is prepared by the receiving device. In light of the specification the Examiner assumes that this is typographical error and that the Applicant intended for the limitation to read: "means for receiving a confirmation request from said *receiving* device". Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1 rejected under 35 U.S.C. 103(a) as being unpatentable over Kirsch et al. US Patent Number () (Kirsch, hereinafter) in further view of Henry US Patent Application # 2003/0182379 (Henry, hereinafter).

As to claim 1, Kirsch teaches:

a system for preventing the delivery of unsolicited and undesired electronic messages comprising (In the Abstract Kirsch teaches a system and method for preventing the delivery of unsolicited emails including a challenge/response feature.):

a sending device sending electronic messages wherein each said electronic message sent by said sending device contains data identifying each said electronic message sent and wherein each said electronic message sent by said sending device contains data identifying the sending device purportedly sending each said electronic message (Paragraph [0066] teaches determining if an outbound email is an original message, i.e. not a challenge message, and if it is appending a "digital signature".);

a receiving device receiving electronic messages, said receiving device communicating with a receiving module (Fig. 1 shows a typical network configuration with computers which can transmit and receive messages.

Paragraph [0029] teaches "inbound e-mail messages are conventionally received in an inbox." It is interpreted that a receiving device is a computer and the receiving module is the software running on the device which has an incorporated inbox.),

said receiving module comprising:

means for temporarily withholding from delivery to the intended recipient an electronic message received by said receiving device (Paragraph [0037] teaches a temporarily pending in-box in Fig2 called the "temp box 36". Also paragraph [0050] teaches "Thus, inbound e-mail 62 directed to a user's e-mail account is initially stored in a temporary queue 64.");

means for locating within said received electronic message data identifying said received electronic message (Paragraph [0011] teaches "in response to the receipt of a predetermined e-mail message from an unverified source address, a signature data key encoding information reflective of some aspect of the predetermined e-mail message.");

means for locating within said received electronic message data identifying the device from which the received electronic message is purported to have been sent (Paragraph [0050] teaches "The received e-mail is evaluated 66 to determine the nominal sender of the received e-mail message. Once the sender is identified, the message is further evaluated.");

means for preparing and transmitting a confirmation request to the device identified as the purported sender of

said received electronic message, wherein said confirmation request contains data identifying said received electronic message (In paragraph [0056] Kirsch teaches sending a confirmation request.);

means for receiving a reply to said confirmation request wherein said reply affirms or denies that said received electronic message was sent by said device identified as the purported sender of said received electronic message (Paragraph [0011] teaches "The computer system then operates to detect whether an e-mail message, responsive to the challenge e-mail message, is received and whether this response e-mail message includes a response key encoding predetermined information reflective of the predetermined aspect of the challenge e-mail message."), and;

means for permitting delivery of said received electronic message to the intended recipient when the reply to said confirmation request message affirms that the device identified as the purported sender of the message sent the message (Paragraph [0059] teaches "For received e-mail messages with valid digital signatures, the message is next examined for a correct response 112 to the cognitive request. If the response is either absent or incorrect, the received email message is again removed 108 from the pending box 30'. When a valid cognitive response is found, the response e-mail is again discarded 108' and the challenge list is again updated 110. Processing continues, however, with the robot effectively switching e-mail accounts

114. This account switch is made to the client e-mail 22 user's account at least to the extent necessary or appropriate to enable the robot to access the pending box 30 of the user account for the purpose of transferring 116 the corresponding challenged e-mail message from the user's pending box 30 to the user's inbox 32."),

said sending device communicating with a sending module and said sending device comprising means for receiving a confirmation request from said receiving module and for communicating said confirmation request to said sending module (Fig. 1 shows a typical network configuration with computers which can transmit and receive messages. Paragraph [0029] teaches "Similarly, e-mail messages originated by the e-mail client system 22' are queued to an outbox 34 to pend delivery to an ISP." It is interpreted that a sending device is a computer and the sending module is the software running on the device which has an incorporated outbox.),

said sending module comprising:

means for locating within each said electronic message sent by said sending device data identifying each said electronic message, wherein said data identifying each said electronic message corresponds to the data identifying said received electronic message included in said confirmation request (Paragraph [0011] defines the signature as "a signature data key encoding information reflective of some aspect of the predetermined e-mail message." Inherent to

appending a key which includes "encoded information reflective of some aspect of the predetermined e-mail message" would be locating the information.);

means for receiving a confirmation request from said sending device (Paragraph [0011] teaches receiving a challenge and responding to it: "This e-mail message, including the data key, is then issued to the unverified source address. The computer system then operates to detect whether an e-mail message, responsive to the challenge e-mail message, is received and whether this response e-mail message includes a response key encoding predetermined information reflective of the predetermined aspect of the challenge e-mail message." The email including the data key is the challenge email that is sent and consequently received. Additionally Fig. 4 shows receiving a challenge response email.);

means for replying to said confirmation request message wherein said reply confirms that said sending device sent the received electronic message when the data identifying said received electronic message contained within said confirmation request message identifies a message sent by said sending device and wherein said reply denies that said sending device sent the received electronic message when the data identifying the received electronic message contained within said confirmation request message does not identify an electronic message sent by said device sending electronic messages (Paragraph

[0059] teaches the reply to the challenge as being received by the receiving device from the sending device. Inherent to receiving the reply would be the transmission of the reply by the sending device. Additionally, the reply includes a response key which is generated according to the sent challenge signature data key. The sent challenge signature data key was generated by "encoding information reflective of some aspect of the predetermined e-mail message". It has already been interpreted that the challenge message contains data identifying the electronic message sent, i.e. the key. It is therefore interpreted that the response key, which is generated from the sent challenge signature data key, is based on information identifying the electronic message sent, since the sent challenge signature data key is based on that information. The response key is sent with the reply and from the response key it is determined if the sender had sent the message.).

Kirsch teaches a method of replying to challenge emails which includes preparing and appending a response key to the reply. In Kirsch's disclosure, the described method of replying to a confirmation challenge email does not make explicit reference of copying and storing the data identifying the electronic messages sent. Kirsch does not explicitly teach:

said sending module comprising:

means for copying and storing said data identifying each said electronic message sent by said sending device and wherein said data identifying each said electronic message copied and stored by said sending device corresponds to the data identifying said received

electronic message included in said confirmation request prepared by said receiving module;

means for comparing the data identifying said received electronic message within said confirmation request with the data identifying each electronic message sent by said sending device and stored by said sending module to determine whether the data identifying said received electronic message in said confirmation request message identifies an electronic message sent by said sending device; and

However, an analogous art, Henry, teaches in Fig. 6 a method for validating emails which are initially considered invalid. Henry teaches the following limitations:

said sending module comprising:

means for copying and storing said data identifying each said electronic message sent by said sending device and wherein said data identifying each said electronic message copied and stored by said sending device corresponds to the data identifying said received electronic message included in said confirmation request prepared by said receiving module (Paragraph [0064] teaches "an HTML (hyper text mark-up language) based email message is sent to the email address thought to be invalid. A unique code is included within the email address, and a record of the code and email address is recorded.");

means for comparing the data identifying said received electronic message within said confirmation request with the data identifying each electronic message sent by said sending device and stored by said sending module to determine whether the data identifying said received electronic message in said confirmation request message identifies an electronic message sent by said sending device (Paragraph [0066] teaches "At block 606, the copy of the code received from the HTML email message is compared to the code sent. Where the code is the same, it is assumed that the email address is functional, and should be reclassified as valid."); and

Therefore, it would have been obvious for one of ordinary skill in the art, at the time of the invention, to combine Kirsch system and method for selectively blocking delivery of electronic mail with Henry's method of validating senders of messages. It would have been obvious to combine the inventions since they both deal with validation of sent messages. Specifically, it would have been obvious to combine since Henry enables the validation of senders to be automated. Paragraph [0005] talks about the problem with most validation systems and how they are not automated. By Henry's method of keeping a record of the sent messages the validation of senders can be done automatically.

As to claim 5, claim 5 is the same as claim 1 except that instead of the system using "data identifying" the electronic message to be confirmed, it uses an identification data string. Claim 5 is rejected in the same manner as claim 1 with the same motivation to combine. Both Kirsch and

Henry teach the information which identifies the sent message as a code or key, i.e. a data string, which has been generated in some fashion, i.e. an algorithm.

All of the limitations which just replace "data identifying" with "identification data string" are rejected for the same reason as claim 1 in further view of:

Kirsch teaches in the abstract that " The origin address of an e-mail message is validated to enable blocking of e-mail from spam e-mail sources, by preparing, in response to the receipt of a predetermined e-mail message from an unverified source address, a data key encoding information reflective of the predetermined e-mail message."

Henry teaches in paragraph [0064] that "a unique **code** is included within the email address, and a record of the code and email address is recorded." This code is also disclosed as being generated, i.e. an algorithm.

The three limitations which were not presented in claim 1 are:

Kirsch teaches means for preparing an identification data string from said received electronic message wherein said identification data string is prepared by applying an algorithm to said received electronic message (Paragraph [0011] teaches "This is achieved in the present invention by providing for the operation of a computer, for the purpose of validating the origin address of an e-mail message to enable blocking of e-mail from bulk e-mail sources, by preparing, in response to the receipt of a predetermined e-mail message from an unverified source address, a signature data key encoding information reflective of some aspect of the predetermined e-mail message.");

Kirsch teaches means for preparing an identification data string for each electronic message sent by said sending device wherein said identification data string is prepared by applying said algorithm to each said sent electronic message (Paragraph [0011] teaches "This is achieved in the present invention by providing for the operation of a computer, for the purpose of validating the origin address of an e-mail message to enable blocking of e-mail from bulk e-mail sources, by preparing, in response to the receipt of a predetermined e-mail message from an unverified source address, a signature data key encoding information reflective of some aspect of the predetermined e-mail message." The process is the same for both the sending and receiving devices.);

Henry teaches means for storing said identification data string for each said electronic message sent by said sending device (Paragraph [0064] teaches that "a unique **code** is included within the email address, and a record of the code and email address is recorded.");

The rejection including motivation to combine still remains the same as the rejection made for claim 1 except that the references teach the above limitations pertaining to the concept of electronic messages being identified by a data string which is generated through an algorithm.

As to claim 8, the combination of Kirsch and Henry teach all of the limitations presented in claim 8. Claim 8 simply has all of the limitations of claim 1 and claim 5 rewritten as a different independent claim. The motivation to combine the limitations which are met by Kirsch and Henry would also apply since the scope of the invention has only slightly changed to include

both representing the data identifying electronic message as data strings created through an algorithm and locating that data within a message.

As to claim 12, Kirsch teaches:

a system for preventing the delivery of unsolicited and undesired electronic messages comprising (In the Abstract Kirsch teaches a system and method for preventing the delivery of unsolicited emails including a challenge/response feature.):

a sending device sending electronic messages wherein each said electronic message sent by said sending device contains data identifying each said electronic message sent and wherein each said electronic message sent by said sending device contains data identifying the sending device purportedly sending each said electronic message (Paragraph [0066] teaches determining if an outbound email is an original message, i.e. not a challenge message, and if it is appending a "digital signature".);

a confirmation device in communication with said sending device (In Paragraph [0058] Kirsch teaches a confirmation device which handles the challenge emails, i.e. confirmation request. "By sending challenge e-mail messages from an alternate or "Robot" e-mail account, challenge response messages are readily segregated from the e-mail stream directed to the user of the e-mail client 22'." It is interpreted that this "robot email

account which processes and handles the incoming messages which will do the validation process of the emails is the confirmation device.);

a receiving device receiving electronic messages, said receiving device communicating with a receiving module (Fig. 1 shows a typical network configuration with computers which can transmit and receive messages. Paragraph [0029] teaches "inbound e-mail messages are conventionally received in an inbox." It is interpreted that a receiving device is a computer and the receiving module is the software running on the device which has an incorporated inbox.),

said receiving module comprising:

means for temporarily withholding from delivery to the intended recipient an electronic message received by said receiving device (Paragraph [0037] teaches a temporarily pending in-box in Fig2 called the "temp box 36". Also paragraph [0050] teaches "Thus, inbound e-mail 62 directed to a user's e-mail account is initially stored in a temporary queue 64.");

means for locating within said received electronic message data identifying the device from which the received electronic message is purported to have been sent (Paragraph [0050] teaches "The received e-mail is evaluated 66 to determine the nominal sender of the received e-mail message. Once the sender is identified, the message is further evaluated.");

means for preparing and transmitting a confirmation request to said confirmation device wherein said

confirmation request contains data identifying said received electronic message and data identifying the device from which said received electronic message is purported to have been sent (Paragraph [0056], Kirsch teaches sending the challenge, i.e. confirmation request, which includes a digital signature. The digital signature includes information pertaining to the message and sender of the message.);

means for receiving a reply to said confirmation request wherein said reply affirms or denies that said received electronic message was sent by said device identified as the purported sender of said received electronic message (Paragraph [0011] teaches "The computer system then operates to detect whether an e-mail message, responsive to the challenge e-mail message, is received and whether this response e-mail message includes a response key encoding predetermined information reflective of the predetermined aspect of the challenge e-mail message."), and;

means for permitting delivery of said received electronic message to the intended recipient when the reply to said confirmation request message affirms that the device identified as the purported sender of the message sent the message (Paragraph [0059] teaches "For received e-mail messages with valid digital signatures, the message is next examined for a correct response 112 to the cognitive request. If the response is either absent or incorrect, the received email message

is again removed 108 from the pending box 30'. When a valid cognitive response is found, the response e-mail is again discarded 108' and the challenge list is again updated 110. Processing continues, however, with the robot effectively switching e-mail accounts 114. This account switch is made to the client e-mail 22 user's account at least to the extent necessary or appropriate to enable the robot to access the pending box 30 of the user account for the purpose of transferring 116 the corresponding challenged e-mail message from the user's pending box 30 to the user's inbox 32."),

said sending device comprising means for transmitting to said confirmation device data identifying each electronic message sent by said sending device wherein said data identifying each said electronic message corresponds to the data identifying said received electronic message in said confirmation request (Fig. 1 shows a typical network configuration with computers which can transmit and receive messages. Paragraph [0029] teaches "Similarly, e-mail messages originated by the e-mail client system 22' are queued to an outbox 34 to pend delivery to an ISP." It is interpreted that a sending device is a computer and the sending module is the software running on the device which has an incorporated outbox. The sending device sends the messages and the "robot email account", i.e. confirming device receives and processes them. See Fig 4.);

Both Kirsch and Henry teach a confirmation device. Henry most accurately teaches the described method used for confirming a device, but does not explicitly teach the confirming device sending the reply. The Examiner shows that Kirsch teaches the confirmation device comprising means for sending the reply:

said confirmation device comprising:

means for receiving a confirmation request from said receiving module (Paragraph [0011] teaches receiving a challenge and responding to it: "This e-mail message, including the data key, is then issued to the unverified source address. The computer system then operates to detect whether an e-mail message, responsive to the challenge e-mail message, is received and whether this response e-mail message includes a response key encoding predetermined information reflective of the predetermined aspect of the challenge e-mail message." The email including the data key is the challenge email that is sent and consequently received. Additionally Fig. 4 shows receiving a challenge response email.);

means for replying to said confirmation request message wherein said reply confirms that said sending device sent the received electronic message when the data identifying said received electronic message contained within said confirmation request message identifies a message sent by said sending device and wherein said reply denies that said sending device sent the received electronic message when the data identifying the received electronic message contained within said confirmation request message does not identify an electronic message sent by said sending device(Paragraph [0059] teaches the reply to the challenge as being received by the receiving device from the sending device. Inherent to

receiving the reply would be the transmission of the reply by the sending device. Additionally, the reply includes a response key which is generated according to the sent challenge signature data key. The sent challenge signature data key was generated by "encoding information reflective of some aspect of the predetermined e-mail message". It has already been interpreted that the challenge message contains data identifying the electronic message sent, i.e. the key. It is therefore interpreted that the response key, which is generated from the sent challenge signature data key, is based on information identifying the electronic message sent, since the sent challenge signature data key is based on that information. The response key is sent with the reply and from the response key it is determined if the sender had sent the message.).

Kirsch however does not explicitly teach storing the sent messages and then consequently comparing the stored data with the confirmation. However in an analogous art, Henry accurately teaches the method of storing the data pertaining to sent messages. Henry shows a method in Fig.6 which validates emails through the Applicant's claimed invention through comparing the confirmation email and the stored data. Henry teaches the following:

said confirmation device comprising:

means for storing said data identifying each said electronic message sent by said sending device and wherein said data identifying each said electronic message copied and stored by said confirmation device corresponds to the data identifying said received electronic message in said confirmation request prepared by said receiving module

(Paragraph [0064] teaches "an HTML (hyper text mark-up language) based email message is sent to the email address thought to be invalid. A unique code is included within the email address, and a record of the code and email address is recorded.");

means for comparing the data identifying said received electronic message within said confirmation request with the data identifying each electronic message sent by said sending device and stored by said confirmation device to determine whether the data identifying said received electronic message in said confirmation request message identifies an electronic message sent by said sending device (Paragraph [0066] teaches "At block 606, the copy of the code received from the HTML email message is compared to the code sent. Where the code is the same, it is assumed that the email address is functional, and should be reclassified as valid."); and

Therefore, it would have been obvious for one of ordinary skill in the art, at the time of the invention, to combine Kirsch system and method for selectively blocking delivery of electronic mail with Henry's method of validating senders of messages. It would have been obvious to combine the inventions since they both deal with validation of sent messages. Specifically, it would have been obvious to combine since Henry enables the validation of senders to be automated. Paragraph [0005] talks about the problem with most validation systems and how they are not automated. By Henry's method of keeping a record of the sent messages the validation of senders can be done automatically. It would be obvious to implement this

automated method on Kirsch's confirmation device to enable the automation of validation and confirmation of email transmission.

As to claim 16, claim 16 is the same as claim 12 except that instead of the system using "data identifying" the electronic message to be confirmed, it uses an identification data string. Claim 16 is rejected in the same manner as claim 12 with the same motivation to combine. Both Kirsch and Henry teach the information which identifies the sent message as a code or key, i.e. a data string, which has been generated in some fashion, i.e. an algorithm.

All of the limitations which just replace "data identifying" with "identification data string" are rejected for the same reason as claim 12 in further view of:

Kirsch teaches in the abstract that " The origin address of an e-mail message is validated to enable blocking of e-mail from spam e-mail sources, by preparing, in response to the receipt of a predetermined e-mail message from an unverified source address, a data key encoding information reflective of the predetermined e-mail message."

Henry teaches in paragraph [0064] that "a unique **code** is included within the email address, and a record of the code and email address is recorded." This code is also disclosed as being generated, i.e. an algorithm.

The only limitation which was not presented in claim 12 but in claim 16 is:

Kirsch teaches means for preparing an identification data string from said received electronic message wherein said identification data string is prepared by applying an algorithm to said received electronic message (Paragraph [0011] teaches "This is

achieved in the present invention by providing for the operation of a computer, for the purpose of validating the origin address of an e-mail message to enable blocking of e-mail from bulk e-mail sources, by preparing, in response to the receipt of a predetermined e-mail message from an unverified source address, a signature data key encoding information reflective of some aspect of the predetermined e-mail message.");

The rejection, including motivation to combine, remains the same for claim 16 as the rejection made for claim 12 except that the references teach the above limitations pertaining to the concept of electronic messages being identified by a data string which is generated through an algorithm.

As to claim 17, a method for preventing the delivery of unsolicited and undesired electronic messages in a network comprising at least one sending device sending electronic messages and at least one receiving device receiving electronic messages wherein each said electronic message sent by said sending device contains data identifying each said electronic message sent and wherein each said electronic message sent by said sending device contains data identifying the sending device purportedly sending each said electronic message, the method comprising the steps of:

Henry teaches preparing, by said sending device, an information record for each said electronic message sent by said sending

device wherein each said information record contains data identifying each said electronic message sent by said sending device (Paragraph [0064] teaches "A unique code is included within the email address, and a record of the code and email address is recorded." The code is the information record which identifies the electronic message which has been sent.);

Henry teaches storing each said information record prepared by said sending device (Paragraph [0064] teaches "A unique code is included within the email address, and a record of the code and email address is recorded." For the record of the code to be recorded it must be stored in some capacity.);

Kirsch teaches transmitting, by said sending device, an electronic message to said receiving device (Fig. 5 step 124);

Kirsch teaches receiving, by said receiving device, an electronic message sent by said sending device (Paragraph [0029] teaches "Inbound e-mail messages are conventionally received in an inbox 30");

Kirsch teaches withholding the delivery to the intended recipient of said electronic message received by said receiving device (Paragraph [0037] teaches "This challenge list 28 may be alternatively provided as separate challenge list 28 data structure or a data store extension 28 of a temporary or pending in-box 36 structure. The pending box 36 may also be implemented logically within the inbox 30 with suitable modification to the otherwise conventional e-mail client system 22' to accommodate the identification of e-mail messages logically residing with in the pending box 36.");

Kirsch teaches locating, by said receiving device, within said received electronic message device, data identifying said received electronic message and data identifying said sending device from which the received electronic message is purported to have been sent, wherein said data identifying said received electronic message corresponds to said data identifying each electronic message sent by said sending device and stored by said sending device in an information record (Paragraph [0011] teaches "by preparing, in response to the receipt of a predetermined e-mail message from an unverified source address, a signature data key encoding information reflective of some aspect of the predetermined e-mail message. This e-mail message, including the data key, is then issued to the unverified source address." Paragraph [0050] teaches "The received e-mail is evaluated 66 to determine the nominal sender of the received e-mail message. Once the sender is identified, the message is further evaluated.");

Kirsch teaches preparing, by said receiving device, a confirmation request wherein said confirmation request contains data identifying said received electronic message wherein said data identifying said received electronic message corresponds to data identifying each electronic message sent by said sending device and stored by said sending device in an information record; transmitting, by said receiving device, said confirmation request to said sending device purported to have

been the sender of said received electronic message (Paragraph [0011] teaches "This is achieved in the present invention by providing for the operation of a computer, for the purpose of validating the origin address of an e-mail message to enable blocking of e-mail from bulk e-mail sources, by preparing, in response to the receipt of a predetermined e-mail message from an unverified source address, a signature data key encoding information reflective of some aspect of the predetermined e-mail message. This e-mail message, including the data key, is then issued to the unverified source address." The challenge response which includes a signature data key encoding information reflective of some aspect of the predetermined email message, i.e. confirmation request, is prepared and sent to the sending device by the receiving device.);

Kirsch teaches receiving, by said sending device, said confirmation request wherein said confirmation request contains data identifying a received electronic message by said receiving device and wherein said data identifying a received electronic message corresponds to data identifying an electronic message sent by said sending device and stored in an information record (Paragraph [0011] teaches "The computer system then operates to detect whether an e-mail message, responsive to the challenge e-mail message, is received and whether this response e-mail message includes a response key encoding predetermined information reflective of the predetermined aspect of the challenge e-mail message." The sending device receives the challenge and then responds back to the receiving device. The sending device must receive the challenge if it is to respond to said challenge.);

Henry teaches comparing, by said sending device, data identifying said received electronic message with data in each said information record to determine whether said received electronic message was sent by said sending device (Paragraph [0066] teaches "At block 606, the copy of the code received from the HTML email message is compared to the code sent. Where the code is the same, it is assumed that the email address is functional, and should be reclassified as valid.");

Kirsch teaches replying, by said sending device, to said confirmation request, wherein said reply affirms that said received electronic message was sent by said sending device when said data identifying said received electronic message identifies an electronic message sent by said sending device and wherein said reply denies that said received electronic message originated from said sending device when said data identifying said received electronic message in said confirmation request does not identify an electronic message sent by said sending device (Paragraph [0011] teaches "The computer system then operates to detect whether an e-mail message, responsive to the challenge e-mail message, is received and whether this response e-mail message includes a response key encoding predetermined information reflective of the predetermined aspect of the challenge e-mail message." It is clearly taught that a response to the challenge, i.e. reply, is received by the receiving device from the sending device. This response

to the challenge includes a response key, i.e. data identifying the received electronic message, and it is determined from the key whether or not it is a valid response.);

Kirsch teaches receiving, by said receiving device, a reply to said confirmation record, and (Paragraph [0011] teaches "The computer system then operates to detect whether an e-mail message, responsive to the challenge e-mail message, is received and whether this response e-mail message includes a response key encoding predetermined information reflective of the predetermined aspect of the challenge e-mail message.");

Kirsch teaches making available for delivery, by said receiving device, said received electronic message to said intended recipient when said reply to said confirmation record affirms that said sending device sent said received electronic message (Paragraph [0059] teaches "For received e-mail messages with valid digital signatures, the message is next examined for a correct response 112 to the cognitive request. If the response is either absent or incorrect, the received email message is again removed 108 from the pending box 30'. When a valid cognitive response is found, the response e-mail is again discarded 108' and the challenge list is again updated 110. Processing continues, however, with the robot effectively switching e-mail accounts 114. This account switch is made to the client e-mail 22 user's account at least to the extent necessary or appropriate to enable the robot to access the pending box 30 of the user account for the purpose of transferring 116 the corresponding challenged e-mail message from the user's pending box 30 to the user's inbox 32.").

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Kirsch's and Henry's methods of validating email messages which have been sent because Henry's teach would allow Kirsch's method to be automated. They both use a challenge response type of validation process, except Henry's method of validation includes storing information regarding the actual messages sent. Kirsch's teaching is more specifically directed to validating an actual sender and is less concerned about validating a particular message. However it would be obvious to combine the two to create a method for validating individual messages because as Henry points out in paragraph [0005] that "Present systems and methods fail to provide automation, and therefore result in poor performance and excessive costs." It would be obvious to combine them to provide automation and reduce costs.

As to claim 24, claim 24 is the same as claim 17, except claim 24 teaches a confirming device which does the step of comparing "data identifying said received electronic message with data in each said information record for said sending device purported to have sent said received electronic message to determine whether said received electronic message was transmitted to said sending device." Claim 24 also differs from claim 17 in that the confirming device is now the device which stores and receives confirmation message and it does so in conjunction with the sending device.

Claim 24 is rejected in the same manner as claim 17 was rejected including the motivation to combine in further view that Kirsch does teach the comparing and other necessary steps done by a confirming device. The examiner notes that the way the claims are drafted, the

confirming and sending device do not have to be separate devices. However the Examiner notes that in Paragraph [0058] Kirsch teaches a confirmation device which handles the challenge emails, i.e. confirmation request. "By sending challenge e-mail messages from an alternate or "Robot" e-mail account, challenge response messages are readily segregated from the e-mail stream directed to the user of the e-mail client 22'." It is interpreted that this "robot email account which processes and handles the incoming messages which will do the validation process of the emails is the confirmation device.

As to claim 2, 9, 13, 18, and 25, the combination of Kirsch and Henry teach all of the limitations of the independent claims 1, 8, 12, 17, and 24. Kirsch further teaches wherein the data identifying said received electronic message by said receiving module comprises the date and time the received electronic message was prepared and the electronic address for the purported sender of said received electronic message and wherein said data identifying each said electronic message sent by said sending device comprises the date and time each said electronic message was prepared and the electronic address for the sender of each said sent electronic message (Paragraph [0033] teaches "An embodiment of the present invention, which may ultimately be preferred, alternately or additively generates the signature as an encrypted text block containing a variety of specific information. This information preferably includes the origination date and time of the challenge

message, the e-mail address used as the destination for the challenge message, and an identifier of the message for which this challenge message was generated.").

As to claim 3, 10, 14, 19, and 26, the combination of Kirsch and Henry teach all of the limitations of the independent claims 1, 8, 12, 17, and 24. Kirsch further teaches wherein the data identifying said received electronic message by said receiving module comprises the date and time the received electronic message was prepared, the electronic address for the purported sender of said received electronic message, and the electronic addresses for the intended recipients of said received electronic message and wherein said data identifying each said electronic message sent by said sending device comprises the date and time each said electronic message was prepared, the electronic address for the sender of each said sent electronic message, and the electronic addresses for the intended recipients of each said sent electronic message (Paragraph [0033] teaches "An embodiment of the present invention, which may ultimately be preferred, alternately or additively generates the signature as an encrypted text block containing a variety of specific information. This information preferably includes the origination date and time of the challenge message, the e-mail address used as the destination for the challenge message, and an identifier of the message for which this challenge message was generated.").

As to claim 4, 6, 11, 15, 20, and 27, the combination of Kirsch and Henry teach all of the limitations of the independent claims 1, 5, 8, 12, 17, and 24. Kirsch further teaches wherein the receiving module further comprises means for encrypting said confirmation request and means for decrypting said reply to said confirmation request and wherein the sending module further comprises means for decrypting said confirmation request and means for encrypting said reply to said confirmation request message (Paragraph [0033] teaches "Other encoding and encrypting algorithms usable with the present invention include MD5, ROT13 and Public Key Encryption".).

As to claim 7, Henry further teaches wherein said sending module further comprises means for including said identification data string in each said sent electronic message (Henry teaches the code being generated and stored for each message sent.).

As to claim 21, The method of claim 17 wherein the method further includes the steps of:

preparing, by said sending device and by applying an algorithm to each said electronic message sent by said sending device, an identification data string for each said electronic message sent by said sending device and including said

identification data string in said information record for each said sent electronic message;

preparing, by said receiving device for said received electronic message, an identification data string for said received electronic message by applying said algorithm to said received electronic message, and;

wherein the step of preparing said confirmation request further includes including said identification data string for said received electronic message in said confirmation request and wherein the step of comparing, by said sending device, data identifying said received electronic message with data in each said information record further includes comparing said identification data string in said confirmation request with each said identification data string in each said information record for each said sent electronic message to determine whether said received electronic message was transmitted by said sending device.

Both Kirsch and Henry teach that the steps for confirming an email sent include a data string which is created through an algorithm:

Kirsch teaches in the abstract that " The origin address of an e-mail message is validated to enable blocking of e-mail from spam e-mail sources, by preparing, in response to the receipt of a predetermined e-mail message from an unverified source address, a data key encoding information reflective of the predetermined e-mail message."

Henry teaches in paragraph [0064] that "a unique **code** is included within the email address, and a record of the code and email address is recorded." This code is also disclosed as being generated, i.e. an algorithm.

In both cases, the steps to confirm an email message inherently include preparing the message with the data string since in the context of Kirsch and Henry, a unique code or key is generated, i.e. data string via an algorithm, is used for the validation and confirmation of email messages.

As to claim 28, The method of claim 24 wherein the method further includes the steps of:

preparing, by said sending device and by applying an algorithm to each said electronic message sent by said sending device, an identification data string for each said electronic message sent by said sending device, and;

preparing, by said receiving device for said received electronic message, an identification data string for said received electronic message by applying said algorithm to said received electronic message, and;

wherein the step of transmitting to said confirming device by said sending device, data identifying each said electronic message sent by said sending device further includes transmitting said identification data string prepared for each

said sent electronic message, wherein the step of preparing, by said confirming device, an information record for each said electronic message further comprises including each said identification data string in each said information record for each said sent electronic message and wherein the step of preparing, by said receiving device, a confirmation request further includes including said identification data string for said received electronic message in said confirmation request and wherein the step of comparing, by said confirming device, data identifying said received electronic message with data in each said information record further includes comparing said identification data string in said confirmation request with each said identification data string in each said information record for each said sent electronic message to determine whether said received electronic message was sent by said sending device.

Both Kirsch and Henry teach that the steps for confirming an email sent include a data string which is created through an algorithm:

Kirsch teaches in the abstract that " The origin address of an e-mail message is validated to enable blocking of e-mail from spam e-mail sources, by preparing, in response to the receipt of a predetermined e-mail message from an unverified source address, a data key encoding information reflective of the predetermined e-mail message."

Henry teaches in paragraph [0064] that "a unique **code** is included within the email address, and a record of the code and email address is recorded." This code is also disclosed as being generated, i.e. an algorithm.

In both cases, the steps to confirm an email message inherently include preparing the message with the data string since in the context of Kirsch and Henry, a unique code or key is generated, i.e. data string via an algorithm, is used for the validation and confirmation of email messages.

As to claims 22 and 29, the combination of Kirsch and Henry teach all of the limitations of claims 21 and 28 respectively, wherein the method further includes the step of appending to said electronic message transmitted by said sending device to said receiving device said identification data string prepared for said electronic message transmitted to said receiving device (Kirsch teaches appending signatures to the outbound messages. Fig. 6 132, paragraph [0061].).

As to claims 23 and 30, the combination of Kirsch and Henry teach all of the limitations of claims 21 and 28 respectively, Kirsch further teaches wherein the step of transmitting a confirmation request by said receiving device further includes encrypting said confirmation request, the step of receiving said confirmation request by said sending device includes decrypting said confirmation request, the step of

replying to said confirmation request by said sending device further includes encrypting said reply, and the step of receiving said reply by said receiving device further includes decrypting said reply (Paragraph [0033] teaches "Other encoding and encrypting algorithms usable with the present invention include MD5, ROT13 and Public Key Encryption".).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Quine, Douglas B. et al., US 20030187942 A1, System for selective delivery of electronic communications;

Katsikas, Peter L., US 20050188045 A1, System for eliminating unauthorized electronic mail;

Fisher, Clay, US 20050172004 A1, Methods and apparatuses for certifying electronic messages;

Mattathil, George P., US 20050144239 A1, EMAIL SENDER VERIFICATION SYSTEM;

Liu, Gary G., US 20050015455 A1, SPAM processing system and methods including shared information among plural SPAM filters;

Thuerk, Keith A., US 20050076090 A1, Method, system, and apparatus for selective automated electronic mail replies;

Wilson, Brian, US 20040015554 A1, Active e-mail filter with challenge-response;

Wallace, Andrew et al., US 20040249901 A1, Challenge response messaging solution;

Singh, Tarvinder P. et al., US 20040148358 A1, Indirect disposable email addressing;

Goodman, Joshua Theodore et al., US 20040003283 A1, Spam detector with challenges;

Goldman; Phillip Y. et al., US 7290033 B1, Sorting electronic messages using attributes of the sender address;

Evans, Alexander W., US 20050198173 A1, System and method for controlling receipt of electronic messages;

Smith, Steven J. et al., US 20050114516 A1, Systems and methods for automatically updating electronic mail access lists;

Backer; Alejandro, US 20070208941 A1, Method and system for authentication of electronic communications;

Tomkow, Terrence A., US 20040230657 A1, System for, and method of, proving the transmission, receipt and content of a reply to an electronic message;

Tomkow, Terrence A., US 20020144154 A1, System and method for verifying delivery and integrity of electronic messages;

Nassiri, Nick, US 20020046250 A1, Certified and registered electronic mail system;

Zhang, Xiao Quan et al., US 20050076220 A1, Method and System for Using a Point System to Deliver Advertisement Emails and to Stop Spam;

Banister, Scott et al., US 20040260778 A1, Electronic message delivery with estimation approaches;

Landsman, Richard A. et al., US 20050055410 A1, Managing electronic messages;

Araujo, Kenneth S. et al., US 20030191799 A1, Apparatus and accompanying methods for providing, through a centralized server site, a secure, cost-effective, web-enabled, integrated virtual office environment remotely accessible through a network-connected web browser.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Kessler whose telephone number is (571) 270-5005. The examiner can normally be reached on Monday through Thursday 7:00 am - 5:30 pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jason Cardone can be reached on (571)272-3933. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MK/

/Jason D Cardone/
Supervisory Patent Examiner, Art Unit 2145